RL-TR-97-176
Final Technical Report
October 1997

INFORMATION WARFARE MODELING I

Southwest Research Institute

Mark Collier

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

19980217 522

DTIC QUALITY INSPECTED 4

Rome Laboratory
Air Force Materiel Command
Rome, New York

This report has been reviewed by the Rome Laboratory Public Affairs Office (PA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

RL-TR-97-176 has been reviewed and is approved for publication.

APPROVED:

ALEX F. SISTI
Project Engineer

FOR THE DIRECTOR: Joseph Camera

JOSEPH CAMERA
Technical Director
Intelligence & Reconnaissance Directorate

If your address has changed or if you wish to be removed from the Rome Laboratory mailing list, or if the addressee is no longer employed by your organization, please notify RL/IRAE, 32 Hangar Rd, Rome, NY 13441-4114. This will assist us in maintaining a current mailing list.

Do not return copies of this report unless contractual obligations or notices on a specific document require that it be returned.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE
October 1997

3. REPORT TYPE AND DATES COVERED
Final Mar - Oct 96

4. TITLE AND SUBTITLE
Information Warfare Modeling I

5. FUNDING NUMBERS
C: F30602-96-C-0084
PE: 62702F
PR: 4594
TA: 15
WU: N7

6. AUTHOR(S)
Mark Collier

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Southwest Research Institute
6220 Culebra Rd
San Antonio TX 78238-5166

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Rome Laboratory/IRAE
32 Hangar Rd
Rome NY 13441-4114

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
RL-TR-97-176

11. SUPPLEMENTARY NOTES
Rome Laboratory Project Engineer: Alex F. Sisti/IRAE/(315)330-3983

12a. DISTRIBUTION AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*
This report documents the results of survey task in which the contractor was asked to identify current Information Warfare (IW) modeling development within the Department of Defense (DoD) and recommend an approach for IW modeling. It involved working with Rome Laboratory to identify their primary interest area in IW Modeling, surveying DoD for ongoing unclassified IW modeling efforts, and defining an IW modeling architecture which Rome Laboratory could use in the future to guide research and development.

14. SUBJECT TERMS
Information Warfare (IW)
Modeling and Simulation
Command and Control Warfare (CCW)
Electronic Warfare (EW)
Information Dominance

15. NUMBER OF PAGES
52

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	SAR

TABLE OF CONTENTS

1. INTRODUCTION

This document is the Final Report for Southwest Research Institute (SwRI), Project No. 10-7948 entitled "Information Modeling I", performed for Rome Laboratory under Contract No. F30602-96-C-0084. The Institute has been tasked to identify current Information Warfare (IW) modeling development within the Department of Defense (DoD) and recommend an approach for IW modeling. This research project involved working with Rome Laboratory to identify their primary interest area in IW modeling, surveying DoD for ongoing unclassified IW modeling efforts, and defining an IW Modeling Architecture which Rome Laboratory could use in the future to guide research and development.

This document is divided into the following sections:

- Background - a brief background of IW and a scope definition for use through out this document.

- Project Objectives - a brief description of the overall objectives of this research project.

- IW Requirements - a description of the basic IW requirements and primary interest area of Rome Laboratory.

- IW Modeling Survey - the summarized results of the IW Modeling Survey. Detailed responses are provided in another section.

- IW Modeling Architecture - a recommended IW Modeling Architecture and plan for research and development.

- Survey Responses - the typed copies of the received survey response sheets.

- Bibliography - a list of documents and briefings reviewed for this research project.

- Original Survey Responses - the original survey responses.

The final report does not include the actual documents and briefings obtained from different organizations developing IW tools and models. Copies of this material can be distributed to Rome Laboratory, but are too bulky to include in the body of the document. In addition, Rome Laboratory is welcome to copies of the collection of articles, briefings (some of which are on-line), and other documents accumulated during the course of this research project. This information is well indexed by the bibliographies provided in this document.

2. BACKGROUND

Information Warfare is a very difficult concept to define. IW consists of a strategy where the information infrastructure of an adversary is disrupted and our friendly information infrastructure is protected. IW defines the concept of "Information Dominance" where friendly forces dominate a conflict by dominating and controlling the information availability, content, and flow. Information, including the forms of command, control, and intelligence is absolutely critical to modern military (and non-military) operations.

Offensive IW attempts to disrupt the availability, quality, and timeliness of information, thus extending the adversary's Observe, Orient, Decide, and Act (OODA) loop process. Defensive IW attempts to protect the same friendly information process from similar disruption, and thus reduce our OODA loop. Much of the development of offensive IW techniques and weapons is highly classified. Development of defensive IW techniques are typically unclassified.

Very few organizations share the same understanding of what IW really is. Some of the most common definitions of IW used within the DoD are:

- Air Force Definition:

  - Any action to deny, exploit, corrupt, or destroy the adversary's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions.

- Army Definition:

  - Actions taken to achieve information superiority by affecting adversary information, information based processes, and information systems, while defining our own information, information based processes, and information systems.

- Command and Control Warfare (C2W):

  - C2W is the military strategy that implements IW on the battlefield and integrates physical destruction.

From a military point of view, IW is often considered to be synonymous with C2W. As defined by joint doctrine, C2W consists of the following:

- Physical destruction - the act of physically destroying an adversary asset, through various means, including precision attacks.

- Electronic Warfare (EW) - the activities such as the use of radar, counter-measures, and other electronic means to detect the adversary, counter their ability to detect friendly assets, and degrade the performance of their systems.

- Operations Security (OPSEC) - the activity whereby the details of friendly operations are secure and prevented from compromise by the adversary.

- Tactical Deception (TD) - the activity of deceiving the adversary through various means to achieve a tactical advantage.

- Psychological Operations (PSYOPS) - the activity of manipulating the morale and mental perception of the adversary through various means.

Each of these aspects (often referred to as pillars) are tied together through integrated use and distribution of intelligence. The availability of timely and accurate intelligence is critical to C2W because more information is needed to effectively exploit and attack the adversary and to assess the effects of operation. The primary actions taken within C2W are C2Attack and C2Protect. C2Attack is an operation where the C2 communication assets and corresponding process of the adversary are attacked, disrupted, and exploited. C2Protect is the converse operation, which involves protecting friendly C2 communication assets from disruption by the adversary.

C2W is primarily focused on disruption (and protection) of the flow of information along C2 lines during a conflict. This is a critical operation, but not the entire spectrum of what IW involves. From a DoD point of view, IW consists of the disruption (and protection) of all relevant information and information flows. IW also includes operations which are not within the responsibility of the DoD. Therefore, C2W is a subset of IW both in terms of functional scope and time (before, during, and after the conflict). Figure 2-1 illustrates this concept.

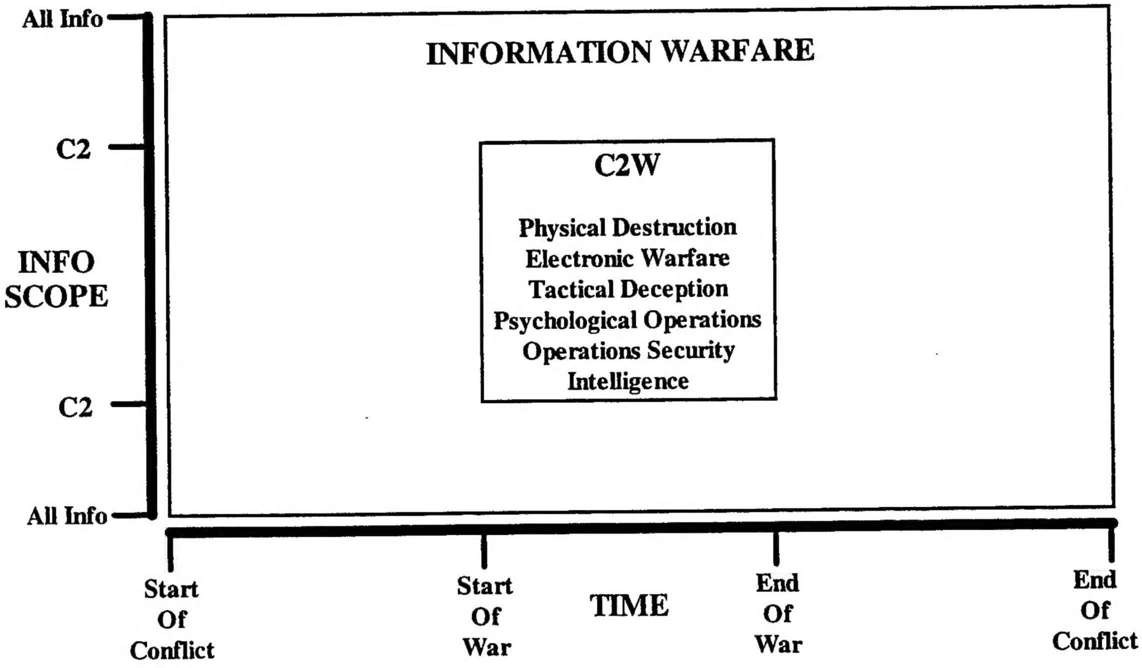


Figure 2-1. C2W Versus IW

To define the scope of IW relevant to the DoD, we must increase the C2W C2 scope to include all information. IW expands the concepts of C2Attack and C2Protect to Information Attack and Information Protect (or Information Assurance). IW also expands C2W in that it considers activities throughout a conflict (before and after a hot war). This definition is consistent with that provided by the Air Force Information Warfare Center (AFIWC).

3. PROJECT OBJECTIVES

The primary objective of this project is to assist Rome Laboratory in better understanding how to model IW. Modeling and simulation is a key to understanding, training, planning, and employing IW for both defensive and offensive needs. To achieve the objectives of this research project, the following major steps were planned:

- Work with Rome Labs to define IW and identify their scope and requirements for IW modeling. The goal of this task is to insure that the recommendations provided by this report are consistent with the funding intentions of Rome Laboratory.

- Conduct a survey to determine the current state of the art in IW model development:

  - Determine which organizations are active in IW modeling.
  - Determine current and planned activity in the area of IW modeling.
  - Determine what needs to be done in IW modeling.

- Define a high-level architecture for an integrated IW model. If possible, define approaches for selected areas which are not being addressed by other DoD centers.

It is not a reasonable objective to attempt to define a modeling architecture for all IW applications. IW is too broad a term and consists of too many applications. Rather the goal is to determine what activity is ongoing, what IW modeling research would be beneficial, and an IW modeling architecture to initiate Rome Laboratory's research in IW modeling.

4. IW MODELING REQUIREMENTS

This research project is not intended to focus on IW requirements definition. A useful future effort would involve working with potential users of IW modeling to determine their requirements. The requirements definition process performed for this research project involved working briefly with Rome Laboratory to understand their primary interest area. Within the Air Force Materiel Command (AFMC), the four Air Force labs are each pursuing different areas of IW. According to Mr. John Pirog, who leads Rome Laboratory's IW group, Rome Laboratory is focusing on defensive IW. Defensive IW is primarily concerned with the concept of C2protect, Computer Security (COMPUSEC), and Information Security (INFOSEC). Much of the non-simulation IW research being performed at Rome Laboratory in the area of IW is in the area of INFOSEC, where work is being performed in technologies such as intrusion detection, recovery, wrappers, survivable information systems, and other efforts.

It is understood that Rome Laboratory will certainly be involved in IW areas outside of those listed above, including some offensive work. This is valuable, because it is not possible to develop defensive IW technology unless the threats to information systems are well understood. However, for the focus of this research project, the basic set of requirements will focus on development of defensive IW Tools.

A primary potential user of technology developed by Rome Laboratory is the AFIWC. The AFIWC is developing both offensive and defensive IW capabilities. From a modeling perspective however, the AFIWC is concentrating more on offensive models, such as those used for target nomination. The AFIWC has a significant effort involving information protect applications, but has not initiated a major defensive IW modeling and simulation effort. The AFIWC is working on this problem and has a working group addressing requirements. This working group is composed of individuals from the AFIWC/Systems Analysis (SA) and AFIWC Engineering Analysis (EA) directorates. It is the Institute's understanding that a request for a FY 99 POM has been submitted, but work up to that time will not be extensive. This provides Rome Laboratory with an opportunity to work to develop defensive IW modeling capabilities which will assist the AFIWC and other DoD organizations.

5. IW MODELING SURVEY

In order to best focus the future IW modeling research effort of Rome Laboratory, it is useful to determine what IW modeling is ongoing within the Air Force and the DoD. The idea is to determine current activity in order to obtain contacts, learn more about IW in general, avoid duplication, and potentially reuse products or collaborate with other organizations.

To scope the survey to a manageable level, only efforts which were clearly IW or C2W were considered. Individual models considering destruction, EW, or other level 1 and 2 models were not considered. Truly unique efforts in the area of level 1 or 2 PYSOPS, TD, or OPSEC models would have been identified, although none were found. It is the Institute's opinion that IW modeling really becomes useful at the levels 3 and 4 where the effect of an IW activity can been reviewed as it affects an overall mission or campaign. IW is also considered to be an integrated strategy using pre-existent and new concepts, which lends itself to higher level, mission or campaign models.

The IW modeling survey was also focused on modeling. There are a number of organizations developing IW capabilities, including databases and defensive IW tools. Some of this information is present in the survey responses, but was not the focus and is not reported in this section.

The basic process for the survey was to identify the appropriate organizations likely to be developing IW models. This was performed by leveraging personal knowledge, literature searches, conference briefings, use of the Internet, and contacting organizations referenced by initial respondents. As potential participants were identified, they were contacted and/or a survey letter was distributed. The survey was conducted at the unclassified level. This prevented several organizations from responding fully or in some cases, responding at all.

This section provides a description of the survey itself, the survey status with a list of the survey participants, a summary of the survey, and a description of the relevant IW modeling activity.

5.1 Survey Description

The survey was intentionally kept brief to encourage participants to respond. The survey was intended to gather basic information about organizations' perceptions of IW and what IW modeling activity is ongoing. The questions included in the survey are listed below:

(1) How would you define the scope of what is or is not an Information Warfare (IW) model?

(2) Describe the basic application of IW modeling used within your organization (target analysis, C2 protect analysis, training, etc.).

(3) Describe ongoing IW modeling activity within your organization.

(4) Describe planned IW modeling activity within your organization.

(5) Describe steps taken or standards used to assist in the reuse of your organization's IW models within other organizations.

(6) Describe IW modeling areas which in your opinion have not been addressed but need to be within the Department of Defense.

(7) List other organizations or points of contact which you know to be involved with IW modeling. If possible, please include name, address, phone number, and electronic mail address.

(8) Indicate whether or not in your opinion, review of active simulation efforts can only be conducted at a high classification level.

5.2 Survey Status

Table 1-1 lists each of the organizations and individuals to which survey letters were distributed. The table includes the organization, the office symbol, the point of contact, whether or not the individual has responded, whether or not IW modeling is ongoing, and notes.

Table 1-1. Survey Results

Org	Office	Contact	Resp	IW?	Notes
AFIWC	CA	Mr. Larry Merritt	NO	YES	Technical director of the AFIWC
AFIWC	AP	Mr. Richard Agopsowitz	NO	YES*	
AFIWC	EA	Mr. John Bres	NO	YES	EA (INFOSEC) M&S POC
AFIWC	OSX	Mr. Mike Ley	YES	YES	Sensor Combat IW war game
AFIWC	OSX	Mr. Jesse Leal	YES	YES	Sensor Combat IW war game
AFIWC	OSX	Capt. Wayne Wooten	YES	YES	Sensor Combat IW war game
AFIWC	OT	Mr. Rich Snook	YES	YES	IW Initiative POC
AFIWC	OT	Mr. Mike Kretzer	YES*	YES	IW Initiative POC
AFIWC	SA	Mr. Jim Oliver	YES	YES	Director of Systems Analysis directorate.
AFIWC	SAA	LtC. Tom White	NO	YES	C2W Analysis Targeting Tool (CATT)
AFIWC	SAA	Mr. Brent Washam	YES	YES	C2W Analysis Targeting Tool (CATT)
AFIWC	SAC	LtC. John Grigus	YES	YES	
AFIWC	SAM	Mr. Bob Eddy	YES	YES	IW DIS/HLA applications

Org	Office	Contact	Resp	IW?	Notes
AFIWC	SAV	LtC. Audenaert	YES	YES	C2Protect requirements
AFIWC	SAV	Rick Higgins	YES	YES	C2Protect requirements
AIA	DOMM	LtC. Paul Bailor	NO	?	AIA POC for M&S
AIA	XRP	Capt. Helen Lento	NO	?	
AIA	XRRT	Mike Tenney	NO	?	
NAIC	TAC	John Tidwell	NO	YES*	CNMT/E lead
RL	C3AB	Mr. John Faust	NO	?	
RL	C3AB	Mr. Joe Giordano	NO	?	
RL	IRDS	Mr. John Pirog	YES	NO	Rome Lab IW lead
RL	IREA	Mr. Alex Sisti	NO	YES*	Rome Lab IW M&S lead
RL	IREA	Ms. Tandi Paugh	NO	YES*	CNMT/E
AL/HSC	XRT	Maj. Terrence Peacock	NO	?	
AL/HSC	XRTH	LtC. William Wimpee	NO	?	
PL	WSC	Maj. Mark DeVirigilio	NO	?	
WL	AA	Maj. Randall Paschall	NO	?	
WL	AAWD-1	Mr. Michael Croner	NO	?	
AF/XOM	XOMT	Capt. Joe Sublousky	YES*	NO	Responded via AFSAA
AF/XOM	XOMW	COL. Ronnie Stanfill	YES*	NO	Responded via AFSAA
AF/XOX	XOXD	Maj. Andrew Weaver	NO	?	
AFSAA		Capt. Kate Kleman	YES	NO	Working on gathering IW information
AFSAA		LtC. Michael B. McGinty	YES	NO	
AF/SC	SC	Maj. Bob Fisher	NO	?	
AF/SC	SCXD	LtC. Garry W. Cole	NO	?	
AF/SC	SCXP	Maj. Mark Lorenz	NO	?	
AF/SC	SCXX	COL. Len Kaplan	NO	?	
AF/SC	SCE	Maj. Stockholm	NO	?	

Org	Office	Contact	Resp	IW?	Notes
AFC4A	TNSCC	Mr. Chet Ratcliffe	NO	?	
AFC4A	TNSC	Maj. Michael Rogers	NO	?	
AFC4A	TNAA	Maj. C.D. Brashares	NO	?	
ACC	DRB	Cliff Gardner	NO	?	
ACC	DRB	Maj. Michael S. Butler	NO	?	
AFMC		Maj. Richard D. Simpson	YES	NO	AFMC IW POC
ASC	XRJ	Arthur W. Daum Mike Hucul	YES	NO	J-MASS project office
ESC	ICJ	LtC. Ken Marvin	NO	?	
ESC	ICJ	Mr. Mike Michelson	NO	?	
ESC	IW	Capt. Chris Anderson	NO	?	
ESC	SRK	Capt. Roy Smith			
ESC	XRR	Mr. Peter Hughes	NO	?	
SA-ALC	LT-D	Mr. Mark Troutman	YES	NO	
SMC	SDAS	Capt. Tom Allison	NO	?	
SSG	EN	Stephen D. Stewart	YES	NO	Defensive IW for AFMC
SMC	XRL	Maj. Patrick Ferrell	NO	?	
AMC	DOU	Maj. Rich Toney LtC. Rob Hall	YES	NO	AMC POC for IW
AFSC	DOXS	LtC. Win Macklin	NO	?	
AFSC	INAJ	Mr. Tim Marburger	NO	?	
AFSOC	INX	LtC. Henry Reimers	NO	?	
AFSOC	XPP	Maj. J. D. Clem	NO	?	
LIWA		COL Halbert F. Stevens	YES*	YES	
LIWA		LtC. Bob Vrtis	YES	YES	LIWA M&S POC for MPRS
LIWA		LtC. Thomas Hudson	YES*	YES	
INSCOM		Mr. Irving Bergman	NO	?	
INSCOM		Col. Ronald Carter	NO	?	

Org	Office	Contact	Resp	IW?	Notes
LMTF		LtC. Jim Kelly	YES	NO	
NGIC		COL. Robert Reuss	YES*	NO	
NGIC		Robert Kenward	YES	NO	Databases TEARS, INNET, SPIRITS
Army HQ		Mr. Phil Loranger	NO	?	
Army HQ		Mr. William M. McDowell	NO	?	
SPAWAR		LCDR. Gerald Burnette	YES*	NO	Passed survey to CDR Slattery
FIWC		CDR. Gerald Mason	NO	NO*	Told by NIWA that FIWC does no IW modeling
NIWA		LCDR. Frank Slattery	YES	YES	NIWA/NRL developing offensive IW capability
NIWA		Ms. Rosemary Wenchell	YES	YES	Developing offensive IW modeling capability
NRaD		Ms. Deb Porter	NO	NO	Developing IWSS
NRaD		Mr. Lee Zimmerman	NO	NO	Developing IWSS
JCS		CAPT. William N. Deaver	NO	?	
JCS		LtC. Jim Weidner	YES	NO	
JC2WC	PD	CAPT. R. Kernan	NO	NO	Previous Information Protect director
JC2WC	PD	CDR. John Primer	NO	NO	Previous Information Protect (ACTD) chief
JC2WC	PD	Mr. Bob Neff	YES	NO	
JC2WC	SIA	Mr. Larry Whatley	YES	YES	CNMT/E applications
JC2WC	SIS	Mr. Brad Boyers	NO	YES	JECEWSI, JNETS, JCAS, JOISIM
JWAC	JN53	Ron Sinek	NO	YES*	Infrastructure modeling
JWFC		LtC. Doug Martin	NO	?	
JWFC		COL Verbeck	NO	?	
DARPA		Dr. Randy Garrett	YES	YES	Stated activity ongoing, but classified
DARPA		Teresa Lunt	YES	NO	ARPA INFOSEC POC
DIA		Mr. Chris Guenther	NO	?	DIA M&S POC
DIA		Mr. Glenn Price	NO	?	Developing IWSS

Org	Office	Contact	Resp	IW?	Notes
DISA	D85	Dr. John Dockery	YES	YES	Cognitive modeling for C4/ISR
DMSO		CAPT. Jim Hollenbach	YES	NO	
DMSO		Dr. Judith Dahmann	YES*	NO	
NSA	R55	Dr. Sid Kissin	NO	YES	NSA M&S POC - developing GCAT
NSA	P42	Mary Johnson	NO	YES	IWSC - Developing Adversary
NSA	P42	Doug Young	NO	YES	IWSC - Developing Adversary
OASD	C3I	LtC Elizabeth Anderson	NO	?	
OASD	C3I	COL Doug Hotard	NO	?	
OASD	C3I	Barbara Valeri	NO	?	
OSD	IPD	Gary D. Guissanie	YES	?	
OSD	IPD	CAPT. Brent Greene	NO	?	
OSD	NA	COL. Scott Rowell	YES	NO	
NDU		Dr. Fred Giessler	YES	NO	
AFSC		COL. George Armstrong	NO	?	
AU		LtC. Rod Winter	NO	?	

In Table 1-1, a “YES” entry in the “Resp” column indicates that the individual has sent in a survey response. A “YES*” entry indicates that they were sent a survey, but deferred the response to another individual in their organization. A “YES*” entry in the “IW” column indicates that even though the individual has not formally responded, it is known that IW modeling is ongoing. Some organizations have indicated a reluctance to participate in the survey due to classification concerns. Similarly, there are other organizations who either could not respond or cannot even be mentioned.

5.3 Survey Summary

This section summarizes the overall responses from the survey. Each of the subsections in this section addresses the overall input for each survey question.

5.3.1 Question 1

How would you define the scope of what is or is not an Information Warfare (IW) model?

Definition of the scope of an IW model varied significantly among the respondents. Definitions ranged from primarily C2W to any model which simulates the impact of manipulating information and the resulting effects on military and non-military operations. As expected, IW and IW modeling have different meanings to different individuals and organizations.

A common response involves use of models which address information and the information flow, as opposed to models looking simply at destruction of physical assets, such as within a communications network. Respondents stressed that IW models require synergy between assets and operations, which implies that an IW model would be a level 3 or 4, where interaction between modeled assets and processes occurs. An IW model must consider the overall system information flow and value. An IW model must also allow evaluation of information time value (information can be useless if it is received too late).

Several respondents referred to cognitive modeling in which the reaction to information is simulated. Certain respondents emphasized cognitive modeling as the key to IW. A general lack of PSYOPS models was also sighted. Cognitive and PSYOPS modeling are inter-related because it is necessary to simulate the human decision/reaction process to operations in order to determine the effectiveness of PSYOPS operations. These models would also be useful to support evaluation of tactical deception operations.

Respondents frequently referenced the importance of different forms of infrastructure. Military operations depend on infrastructure, which consists of civilian assets (communications, electrical power, other utilities, etc.) and information systems supporting operations.

Some respondents expressed IW primarily in terms of C2W and forsee modeling opportunities for individual pillars of C2W. Some respondents stated that existing EW and C2W models could be used to perform IW operations, but in themselves are probably not IW models.

One response stated that IW modeling will primarily occur via constructive simulations.

5.3.2 Question 2

Describe the basic application of IW modeling used within your organization (target analysis, C2 protect analysis, training, etc.).

As expected, the responses to this question varied based upon the role of the organizations. Some of the applications of IW modeling expressed by respondents include:

- Decision aids and analysis tools (what if tools).
- Battle staff training.
- Training at the tactical, operational, and strategic levels.
- Doctrine development.
- Mission planning and rehearsal at all levels.
- Target analysis.
- Integrated Air Defense System (IADS) analysis.
- Test and evaluation.
- Acquisition of IW weapons.
- Infrastructure (information and otherwise) dependence analysis.
- Outgrowth of EW.
- Jamming of key links, signal detectability, etc.

- Security policy.
- Red team planning.
- Education, trend projection, issue identification, consciousness raising, and policy.

5.3.3 Question 3

Describe ongoing IW modeling activity within your organization.

Overall, the current level of IW modeling activity is limited. Much of the existing modeling is more C2W than IW. Some of the current activity includes:

- C2W Analysis Targeting Tool (CATT) IADS simulation.
- Sensor Combat campaign level war game.
- IW Initiative architecture for offensive IW.
- Preliminary work on C2 Protect modeling.
- Communication network modeling applications (CNMT/E and GCAT).
- Target nomination models (Adversary).
- Engagement analysis.
- Level 1 and 2 models used for IW purposes.
- IW/C2W Mission Planning Rehearsal Systems (IW MPRS).
- NRL Effectiveness of Navy Electronic Warfare Systems (ENEWS).
- Red/Blue force communication's system models.
- High-fidelity propagation models.
- Detailed communication network model of military C2W structure.
- Radio Frequency Mission Planning (RFMP).
- Cognitive modeling.
- C2W training models (JECEWSI, JNETS, JCAS, and JOISIM).

5.3.4 Question 4

Describe planned IW modeling activity within your organization.

Much of the planned activity is an extension or enhancement of ongoing efforts. Some of the new efforts include:

- Additions to models described above.
- C2 Protect model development.
- Introduction of IW to Distributed Interaction Simulation (DIS)-based exercises.
- Mission rehearsal models.
- Intelligence system model.
- Red and blue Sensor-to-Shooter process modeling
- Risk management models.
- IW attack models.
- IW Synthetic Support Environment (IW-SSE).

5.3.5 Question 5

Describe steps taken or standards used to assist in the reuse of your organization's IW models within other organizations.

Some of the steps taken to improve reuse of models include use of the following:

- Standard interfaces to national models including AWSIM/NASM.
- Ada, C++, and C languages.
- DIS.
- High Level Architecture (HLA).
- Joint Modeling and Simulation System (JMASS) environment.
- Common Object Request Broker Architecture (CORBA) Level 2.0 Standard.
- INTELINK.

5.3.6 Question 6

Describe IW modeling areas which in your opinion have not been addressed but need to be within the Department of Defense.

Several respondents indicated they feel that there are no existing IW models at this time, so they feel the area is wide open. Others pointed out a need for the following types of models:

- Psychological factors, such as morale.
- C2 Protect, COMPUSEC, INFOSEC.
- Additional IADS modeling (process oriented).
- Model logical/physical flow of data together in order to measure the time-value of information.
- Simplistic, yet functional models, accuracy is not always needed.
- Vulnerability analysis of friendly and enemy C4I infrastructure.
- Both civilian and military mapping.
- Battle damage assessment of enemy and friendly forces.
- Modeling of the infrastructure which supports information flow.
- Perception management.
- Computer network attack.
- Affecting enemy decision cycle (both friendly and enemy).
- PSYOPS models.
- Behavioral modeling.

5.3.7 Question 7

List other organizations or points of contact which you know to be involved with IW modeling. If possible, please include name, address, phone number, and electronic mail address.

The results of this question are summarized in Table 1-1.

5.3.8 Question 8

Indicate whether or not in your opinion, review of active simulation efforts can only be conducted at a high classification level.

Many respondents expressed a desire for models to be unclassified or classified as low as possible to allow wide distribution and use. Respondents also indicated that details, specifics, and actual data can be omitted from models in order to allow them to remain unclassified. Often models are not classified; however, the data used for simulation can be highly classified.

Respondents indicated that offensive IW development is naturally highly classified, while defensive IW techniques are not.

There is definite disagreement as to whether an unclassified survey can address true IW modeling. There appears to be a classified community working the truly new IW techniques. Individuals aware of this activity typically indicate that unless these techniques are referenced, you cannot model IW appropriately. Others disagree, but they are perhaps not aware of the activities within this community. The activities that are more widely known and unclassified are the more traditional C2W applications.

5.4 Activity Summary

This section describes ongoing IW/C2W modeling activity which has been identified during the survey. The information is organized in the same order as previously presented in the survey status summary. Included is the Point of Contact (POC) and an indication as to whether or not additional briefing material is available.

5.4.1 Sensor Combat - AFIWC

POC AFIWC/OSX - Mike Ley
Briefing Available

Sensor Combat is a campaign-level IW/C2W model used for IW education, training, and mission planning. Sensor Combat is designed to allow a user to use IW at a strategic level in order to review the results throughout the scenario. Sensor Combat is designed to model many assets within a campaign at an appropriate level of fidelity in order to demonstrate impact to the overall campaign.

Sensor Combat is currently being implemented in the form of two prototypes set in different scenarios. The AFIWC is developing both Korean and Bosnian scenarios. The Korean scenario stresses a "hot" war in which C2W (physical destruction, EW, tactical deception, PSYOPS, OPSEC, and intelligence are modeled). The Bosnian scenario is focusing on more of a peace time campaign with "soft" IW activities such as terrorism and the media. Both scenarios are being developed for PC platforms running Windows 95 or Windows NT.

A usable prototype is expected to be available in mid Fiscal Year (FY) 97. Production versions of the scenarios will be available at the end of FY97.

Sensor Combat has several planned off-shoots including:

- Sensor Cover - An intelligence simulation.
- Sensor Spook - A C2protect simulation.

5.4.2 IW Initiative - AFIWC

POC AFIWC/OT - Mike Kretzer
Briefing Available

The IW Initiative is a multi-year effort involving the development of an architecture and set of tools which will be used as a decision aid for offensive IW. The IW Initiative consists of hardware, networking equipment, Commercial-Off-The-Shelf (COTS) software, and custom software.

The IW Initiative involves an end-to-end architecture in which objectives are input, models are executed to assess target criticality and vulnerability, and then targets are passed through to the Air Tasking Order (ATO) generation process. The IW Initiative integrates near-real-time input of intelligence and IW Battle Damage Assessment (BDA) to allow the decision process to maintain situational awareness.

The IW Initiative is not a model, but rather an architecture and a process which will be populated with various existing and new models. The IW Initiative is not expected to be one large monolithic model, but rather by providing access to a number of models, it will provide processing threads which the user will select based on needs. One such thread is being prototyped at this time.

5.4.3 C2W Analysis Targeting Tool (CATT) - AFIWC

POC AFIWC/SAA - LtC. Tom White
Briefing Available

A detailed IADS simulation incorporating various IADS functions into an overall process model, including target detection, tracking, decision making and engagement, along with communication and identification processes.

CATT is currently the initial model being integrated into the IW Initiative architecture to demonstrate the concept.

5.4.4 DIS IW Integration - AFIWC

POC AFIWC/SAM - Mr. Bob Eddy

Intelligence, engagement, and IADS models are being updated to use DIS to allow introduction of better EW and intelligence to exercises. This activity is a means of adding C2W/IW to distributed exercises.

5.4.5 C2 Protect Modeling - AFIWC

POC AFIWC/SAV - Mr. Rick Higgins

Preliminary work is being performed to develop new C2 Protect models. AFIWC/SAV is currently developing requirements in conjunction with the AFIWC/EA directorate, which is the INFOSEC/COMPUSEC group. Some C2 Protect model investigation or development will occur during FY97.

5.4.6 Communications Network Modeling Tool (CMNT/E) - NAIC

POC NAIC/TACC - Mr. John Tidwell

CNMT/E is a modeling tool which allows dynamic simulation of the physical hardwired communications and logical C2 networks. CMNT/E can be used as a targeting tool in which nodes are selected based on the response of disruption of a node.

CNMT/E uses the Spatial Display Tool (SDT) as its user interface and is based upon CACI's COMNET for the dynamic network simulation.

5.4.7 IW/C2W Mission Planning and Rehearsal System (IW/C2W MPRS) - LIWA

POC LIWA - LtC. Bob Vrtis
Briefing Available

The IW/C2W MPRS is intended to support IW/C2W training during joint exercises. The LIWA is proposing to develop the land component of a larger system that will be integrated with components from other services and joint IW/C2W models from the Joint Command and Control Warfare Center (JC2WC) (namely JCCWSS/JOISIM).

5.4.8 Naval Information Warfare Activity - NIWA

POC NIWA/NRL - Rosemary Wenchell
POC NIWA CDR - Frank Slattery

NIWA established an analysis center, the Naval Information Warfare Analysis Center (NIWAC) on 12 Dec 1995, to provide an expert IW analysis and modeling and simulation (M&S) capability in support of complex management decisions at all levels, and to act as the Navy's technical agent for M&S activities supporting IW applications.

The NIWAC will have the capability to provide high-fidelity engineering/engagement (Level 1/2) IW/C2W support for varied aspects of the DoD functional M&S support areas (acquisition, analysis, training), but will focus its initial efforts on acquisition and analysis.

The NIWAC will provide support in the analysis areas of mission planning, operational planning/support, nodal analysis, vulnerability assessments and mission support. Training support by the NIWAC to the Fleet Information Warfare Center (FIWC) and the Joint Training, Analysis and Simulation Center (JTASC) will be an outgrowth of models initially developed for analysis and acquisition efforts.

Ongoing M&S efforts by the NIWAC are mainly focused on providing support for NIWA's acquisition, development and operational activities and establishing protocols with external organizations. The NIWAC is building the expertise to provide analysis, studies and M&S tools for every phase of a NIWA's system development cycle from acquisition to operations.

The NIWA is expanding the Naval Research Lab (NRL) Effectiveness of Navy Electronic Warfare Systems (ENEWS) visualization and simulation package to include C2W networks and systems. This package will be used as a mission planning tool for some of NIWA's classified projects.

Models of Red and Blue force communication's system are being developed at the design and engineering level. These models will allow for analysis of system vulnerabilities, effectiveness and operational capabilities.

High-fidelity propagation models are being used and enhanced for use in a variety of simulation packages and studies. Environmental effects have a critical impact of the electromagnetic spectrum and communications.

A detailed communication network model of military C2W structure, down to the packet level is being developed for mission planning, vulnerability assessments, nodal analysis and mission support.

The Radio Frequency Mission Planning (RFMP) has been developed and deployed onboard Navy aircraft carriers and at fleet support activities. RFMP is an M&S tool that allows for visualization of the RF environment in support of communication system mission planning and operations. RF propagation models and terrain data are used to calculate environmental effects on friendly and hostile communication links.

5.4.9 CNMT/E and C2W Applications - JC2WC

POC JC2WC/SIA - Mr. Larry Whatley

The System Integration Applications (SIA) Division of the JC2WC is responsible for development of applications and engineering level models for use within the JC2WC and external organizations. The JC2WC is planning to integrate the CNMT/E model, the Simulation Display and Analysis System (SIMDAS), and the Rapid Application of Air Power (RAAP) tool. CNMT/E is a communications modeling tool. SIMDAS provides level 1 and 2 radar and communication models. RAAP is a target management tool. The resulting integrated tool will allow modeling of IADS and other networks.

The JC2WC is currently working on enhancements to CNMT/E and software infrastructure to support integration of these tools and the required databases.

5.4.10 JECEWSI/JNETS/JCAS/JOISIM - JC2WC

POC JC2WC/SIS - Mr. Brad Boyers

The System Integration Simulation (SIS) division of the JC2WC is responsible for development of force level models. The JC2WC is developing a set of models which will eventually replace the current Joint Electronic Combat Electronic Warfare Simulation (JECEWSI) with a new set of integrated models which support training for C2W. The models being developed are:

- JECEWSI - being enhanced and integrated with other models.
- JNETS - network and infrastructure model.
- JCAS - targeting model.
- JOISIM - information (intelligence) model.

JECEWSI is currently integrated via the Aggregate Level Simulation Protocol (ALSP) within the ALSP confederation of models. The new models will become the C2W portion of the Joint Simulation System (JSIMS).

5.4.11 C4/ISR Model - DISA

POC DISA/D8 - Maj. Knowles
Briefing Available

The C4/ISR model is a next generation simulation which models the information cycle within the C4 domain. The C4/ISR model includes IW aspects in which components in the C4 structure are destroyed/downgraded. Effects are also planned for use of psychological operations/deception. Plans are to develop a prototype using the HLA Run Time Infrastructure (RTI) and integrate with JWARS. Eventual integration with JSIMS is also planned.

5.4.12 Cognitive Modeling - DISA

POC DISA/D85 - Dr. John Dockery

Dr. Dockery defines IW as any activity that interferes with human cognition. Dr. Dockery is working on models which simulate the human cognitive and reasoning process. These models will be used to simulate how a commander perceives and reacts to IW, in the sense of how information manipulation affects actions. The models will consider cultural biases, which radically affect how different people react. A product called O-INCA is being used for this effort.

Work is also being performed using STELLA to model how a computer virus interacts with an operating system. This model will be used to assist in development of more virus resistant operating systems. Operating systems are good virus targets because they are so structured and predictable.

5.4.13 Adversary - NSA

POC NSA/P42 - Doug Young
Briefing Available

Adversary is an analysis tool used to determine critical nodes in a communication network. Adversary maintains its own database of communication node and link information. Adversary is based upon the OILSTOCK-based mapping tool which displays links and nodes and allows users to selectively disable nodes and view the downstream effects on communication ability. Adversary visually models the physical communications structure, but does not actively simulate effects. Disabling of nodes is strictly binary.

5.4.14 Generalized Communications Analysis Tool (GCAT) (NSA)

POC NSA/R55 - Dr. Sid Kissin

GCAT is a communications modeling tool similar to CNMT/E. More information has been requested for GCAT.

6. IW MODELING ARCHITECTURE

The final task of this research project is to define an approach or architecture that Rome Laboratory can use for future IW modeling activity. A primary goal is to avoid duplication of existing or near term IW modeling activity. The IW modeling survey indicates that limited IW modeling activity is ongoing; therefore, there is sufficient opportunity to perform research in new areas.

6.1 Background

While there is a great deal of interest in development of offensive IW techniques, a more significant problem lies on the defensive side. Our current military and the civilian infrastructure upon which it depends, is highly vulnerable to IW attacks. The U.S. military is the most information aware and dependent military in existence and is thereby the most lucrative potential target of IW. Research is required to develop capabilities which aid the ability of the military in their understanding of and planning for the IW threat.

It is the Institute's opinion that what makes IW so interesting is that the military and society, in general, are increasingly dependent upon information. The information is becoming so prevalent and accessible through the incredible explosion of network-connected computer systems. Computers and networks are everywhere from individuals' homes to smart weapon systems. These computers store vast amounts of information and the systems/users that use them depend on that information. If one is to concentrate on IW, the focus should be on computer networks and information systems, because they are the nervous systems of our military and society and are becoming the predominant repositories, transmitters, manipulators, and generators of information. This process is continuing at a rapid pace as more and more processes are becoming automated (or at least partially dependent upon automation).

Modern military systems and information-based operations are highly complex. It is very difficult, if not impossible, to manually analyze the result of threats and loss of service when applied to highly complex networks of computers and information. Modeling and simulation is a logical tool to use to analyze this problem. It is the Institute's opinion that the most compelling application of simulation to IW is to develop functional models of large, complex, computer-dependent networks and view the affects of IW attacks on the overall ***information-based operational processes*** using the network. The resulting models and simulations must go beyond current "critical node" and "choke point" tools in supporting analysis of the impact of IW attacks on a node or specific information component. The models must simulate the information flow (i.e., the Air Tasking Order generation) with representation of the information value in terms of content and time.

Current communication network models focus primarily on identification of critical nodes. Such tools, while useful, suffer from the following limitations:

- The tools do not represent the dependence of networks on infrastructure, computers, and individual information sources.

- The tools do not indicate the impact to the information flow (including value and time) which represents the actual function of the links and nodes in transmitting information relevant to an operational need.

Current "IW" modeling tools are primarily focusing on C2W. These tools are primarily used to represent the physical model of a communications network and then allow the user to identify critical nodes. More recent efforts are expanding the physical models to include specific logical models such as Command and Control (e.g., CNMT/E merges the physical network model with the C2 model as defined by the CONSTANT WEB database). Other models such as CATT focus on C2W for a specific application (in this case being an IADS). Other organizations are performing similar work within focused C2W domains. These statements are not intended to decrease the value of these models. The models identified will be useful for the intended purpose and are appropriate for the organizations developing them; however, it is clear that new models and simulations are required to address the larger IW problem.

The reason the military defends nodes and communication links, or attempts to attack and exploit adversary nodes, is not so much for their intrinsic value, but rather to destroy or disrupt the related information and its flow. Replacing hardware and links, while perhaps expensive, is a relatively straight-forward task. Replacing information is much more difficult. Replacing time lost is impossible. The real intent of defensive IW is to prevent the adversary from disrupting, corrupting, or manipulating the information flow, thereby increasing the time required to make decisions or causing poor decisions to be made (through perhaps deception and psychological operations).

Most information-based processes involve feedback loops in which a process is performed (i.e., as ATO generation and execution), feedback is obtained (BDA), and the process is repeated. These feedback loops can also be described as the Observe Orient Decide and Act (OODA) loops. Defensive IW attempts to reduce, to the maximum extent, the OODA loop times of friendly forces. Conversely, offensive IW attempts to extend the OODA loops of the adversary. The most useful IW model will be one which allows a user to understand and view the assets he uses to support information processes and assist in the identification of critical and vulnerable points. This tool will predict how a network could be most effectively attacked, thereby allowing the user to wisely invest resources for security, survivability, and recovery.

6.2 Overview

The focus of an IW model should be upon identifying the effects of IW on large, computer-dependent networks which support operational processes. The tangible product provided will be an IW modeling tool which will provide the following capabilities:

- Network Structure Visualization - simple visual modeling of the structure of the network and the information flows using the network.
- Vulnerability Analysis - manual and computer-assisted determination of the vulnerability of an information-based process, due to critical nodes.
- Information Flow/OODA Loop Analysis - assessing the impact of an attack on an individual or overall OODA loop.
- Course of Action Analysis - based upon a threat and potential consequence, analysis of the best approach to maximize operations and minimize risk.
- Knowledge Base Creation - the tool could be used prior to conflict to build a rule base which could later be used to assist in an autonomous reaction to threats.

The IW modeling tool to be developed will be designed for defensive IW analysis. The IW modeling tool is one which could be directly used by individuals responsible for a computer/communications network. The data and models within the tool will be designed to support vulnerability assessments, as opposed to performance or other assessments.

The IW modeling tool is intended to assist the users responsible for computer/communication networks in assessing vulnerabilities. The vulnerabilities will be identified from a point of view of which hardware or data assets are the most critical from an information process (as opposed to strictly hardware) point of view. The tool is not designed to assist in identifying particular, individual weaknesses in a network. While this is a useful operation, it is best conducted (at least from a computer point of view) using tools such as SATAN or ICEPICK. The tool is also not designed to model, in detail, the specific interaction of a threat with the target system (such as a virus versus a particular operating system). Again, this can be determined in a controlled environment using real threats and systems. These are important applications, but not compelling from a modeling point of view. Modeling is most appropriate in situations where it is not practical to analyze a problem using real systems. Assessing the impact of losing nodes, links, or data, in a large network to an information-based process, is not possible without the use of simulation.

The IW modeling tool will consist of an underlying architecture which will also support offensive IW analysis. The major difference between a defensive and offensive IW tool of this type is the database used to populate it. If the blue data is replaced with red/gray data, then with some straight-forward user interface changes, the tool could be used for offensive operations such as target nomination.

The remainder of this section provides more detail on the definition of the IW modeling tool. Note, that thought was originally given to development of a higher level IW modeling architecture (or framework). However, since there are other on-going efforts in that area, such as the AFIWC's IW Initiative, developing another such architecture did not seem appropriate. The IW modeling tool described herein is an architecture which will be populated with data, models, and other supporting tools.

6.3 System Architecture

The architecture of the IW modeling tool will consist of a collection of databases, models, and applications. The data, models, and applications will be connected through a standard interface to simplify integration and to allow access by external applications. Figure 6-1 provides a high level block diagram of the architecture.

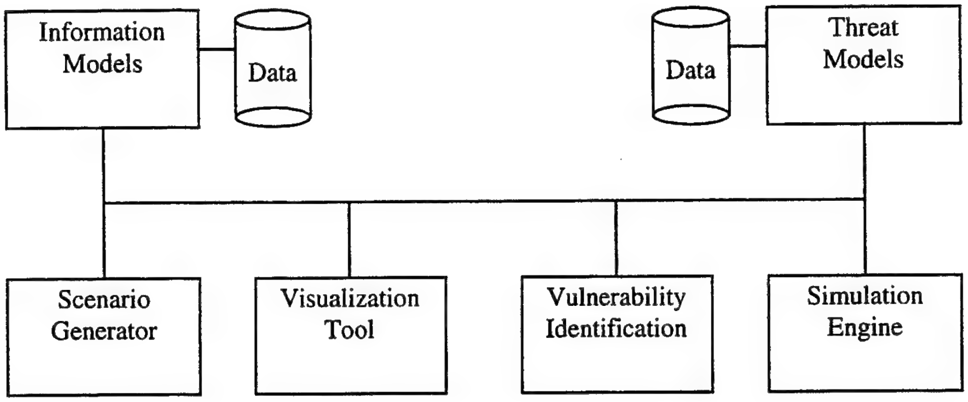


Figure 6-1 - System Block Diagram

The interfaces used will depend on whether or not existing applications can be used. The recommended interface is to take advantage of Object Request Broker (ORB) technology, which allows development of distributed objects. Another advantage of ORBs is that significant ongoing DoD developments are based upon this technology.

The primary databases and models for the IW modeling tool include the following:

- Information Models - the models and data which comprise the network hardware, data, and processes used to transfer information.

- Threat Models - the models and data used to represent threats to the network and information.

These models, particularly the Information Models and the data used to populate the models are the key to the system. Once developed, a variety of applications can be created to utilize the models. The recommended set of applications includes the following:

- Scenario Generator - a GUI tool used to populate the data in the Information Model. Also included will be filters which convert existing data bases to the required format.

- Visualization Tool - an integrated GUI which allows spatial display of the data in the Information Model. The Visualization Tool will also be used by the Scenario Generator to assist in data input and by simulation tools to display results.

- Vulnerability Identification - a manual and automated tool which assists the user in identifying critical and vulnerable parts of the network.

- Simulation Engine - an engine which is used by the vulnerability identification application to determine critical and vulnerable nodes. The simulation engine will also provide an interface to use with external simulations.

The models and applications listed above are described in following sections.

6.4 Information Models

The keys to the IW modeling tool are the information models and scenario databases. These models and databases are the basis for simulation tools which allow the user to perform a variety of "what if" questions. The Information Model is based upon three conceptual models which represent information connectivity/dependency, information value, and information flow. These three types of information models are described as follows:

- Information Connectivity Model (ICM) - the basic connectivity model of computers, networks, infrastructure, and communication nodes which provide the repositories and paths whereby information travels. The ICM describes the network and its dependencies on computers and infrastructure. Models and data for this information already exist, but are spread across several organizations. The ICM defines the ***physical*** layer. There could be many separate ICMs, but only one is expected for any given user scenario (although the user could have multiple scenarios within their area of responsibility).

- Information Value Model (IVM) - the model of the information provided by nodes in the ICM. While much of the ICM exists to transmit information, many of the nodes serve the purpose of adding value to the transmitted information. The IVM represents the individual information sources and dependencies associated with selected nodes. The IVM defines the ***static information*** layer. There will typically be one IVM per ICM.

- Information Flow Model (IFM) - the process associated with the flow of information through the ICM and using the IVM. The IFM consists of templates which represent the flow of information for any number of operational processes. Examples of information flows are the paths taken and data used for intelligence, targeting, ATO generation, etc. The IFM defines the ***dynamic process*** layer and introduces the time value of the information. There will be many separate IFMs for any given user scenario. Information flows are defined as feedback loops (OODA loops). Feedback loops allow the overall/cumulative effect of an attack to be assessed. The information flow templates will be modular and hierarchical to allow subordinate processes to feed larger processes.

From a software implementation point of view, it may not be practical or possible to clearly separate the three models. The models may merge into a basic information model. The three models are used, however, to highlight the types of data and relationships which must be researched and represented in order to support the development of IW modeling tools.

The ICM, IVM, and IFM conceptual models will be implemented in such a way that can be expanded as additional detail is required in the model. The ICM, IVM, and IFM will require an object-oriented structure for representing the complex information structure. The exact architecture may be either entirely custom or based upon a COTS package, if possible. It is essential that this architecture be easily expandable, because as interest and computing capability grows, more details and attributes will be added. Addition of attributes must not affect existing models or the database.

The Information Models are not envisioned to be extremely data intensive. It is not appropriate to develop models which require data which is not practical to obtain. It is also not practical to build models which are so complex that only a very limited set of users can effectively execute them. Rather, it is the intent to develop simplistic functional models which can be expanded in the future if necessary.

6.4.1 Information Connectivity Model (ICM)

The ICM is the foundation model. The ICM is the physical representation of the network and the dependencies (and could alternatively be described as a dependency model). The ICM will consist of an object-oriented structure which will allow expression and expansion of the attributes relevant to the model, such as link and node data and dependency information (for example, the dependence of a radar site on a computer, which depends on a server, which depends on electrical power). A key capability of the ICM is expandability. As IW becomes more widely accepted, the level of detail in the ICM will increase and the data model will have to support expansion without invalidating existing data. Figure 6-2 illustrates the basic ICM concept.

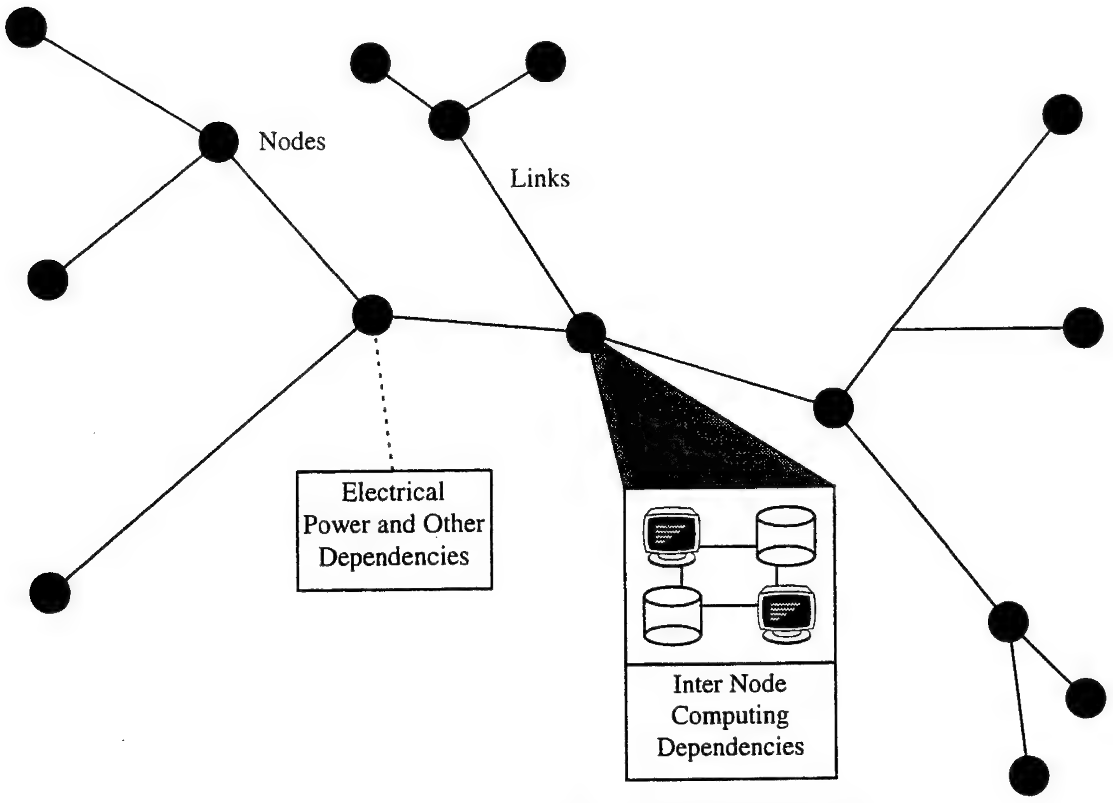

Nodes
Links
Electrical Power and Other Dependencies
Inter Node Computing Dependencies

Figure 6-2 - Information Connectivity Model

The ICM is intended to be an extension of existing physical communication and infrastructure models. There are two primary efforts required to build the ICM:

- Data model - the software and database structure which represents the data and is used to access the data for simulation and visualization.

- Data - the actual data used to populate the model.

While a number of such models already exist, they are present in separate databases and use different software to access and manipulate the databases. Existing databases must be reviewed and software generated or reused to represent the data model portion of the ICM. Some of the databases and corresponding information models to be examined include:

- Adversary (NSA)
- Links and Nodes (NAIC)
- TEARS, INNET, and SPIRITS (NGIC)
- Sensor Harvest (AFIWC)
- Infrastructure Models (JWAC)
- Numerous others

These databases are primarily used to represent red/gray information. While this will not affect the data model, the actual data in the databases will not be useful, unless the ICM is used for offensive IW. Another limiting factor is that the data present in these databases is highly classified and any resulting combination of the data will carry the highest classification level.

Effort is required to identify databases which could be used to populate the ICM. It is necessary to determine what data can be realistically obtained at this time. The availability of data will dictate the structure of the data model, because it is not realistic to base the model on data which is not available. This is very important, because there are attributes which if available, will be of great use within a defensive IW modeling tool. For example, when assessing the threat posed to a computer network by a virus, detailed data on operating systems, patch levels, and known security risks will need to be known. Data which represents the current structure of the network (including computers, routers, bridges, switches, etc.) is also required. Unfortunately, such data is typically very difficult to come by.

Following is an object hierarchy with example attributes maintained within the ICM:

- Node type (link, node)
- ID
- Location[2]
- Recovery/Replacement/Repair time

- Link
  - Transmission type (cable, fiber, RF)
  - Frequency, power, etc.
  - Protocol

- Node
  - Node Type
  - Connections[n]
  - Dependencies[n]
  - Redundant/backup system

  - Computer System
    - Computer type
    - Operating system
    - Patch level
    - Firewall
    - Internet access

  - Communication Equipment
    - Type (Router, switch, etc.)

  - Required Infrastructure
    - Type (Power)

The ICM will support applications beyond those defined for the IW modeling tool. Many offensive and defensive IW applications require a good network connectivity model. A related effort, that will be useful, will be to develop or integrate tools which will automatically generate the ICM based upon the network topology of a user's network. The availability of such tools will simplify development of the ICM for a given scenario and better insure that the data used for the model is up to date.

6.4.2 Information Value Model (IVM)

The IVM builds upon the ICM by adding the relevant information dependencies and assets in the network. The IVM describes the actual "soft" information assets which are present within the network. The IVM is the model which takes the physical network to a higher level where the information is identified.

In order to determine the effects of loss, degradation, or eventually manipulation of information, it is necessary to construct a model which represents the information provided by the nodes of the network. Some of this information is resident in computer systems and some will be introduced through human interaction. Figure 6-3 illustrates the basic IVM concept.

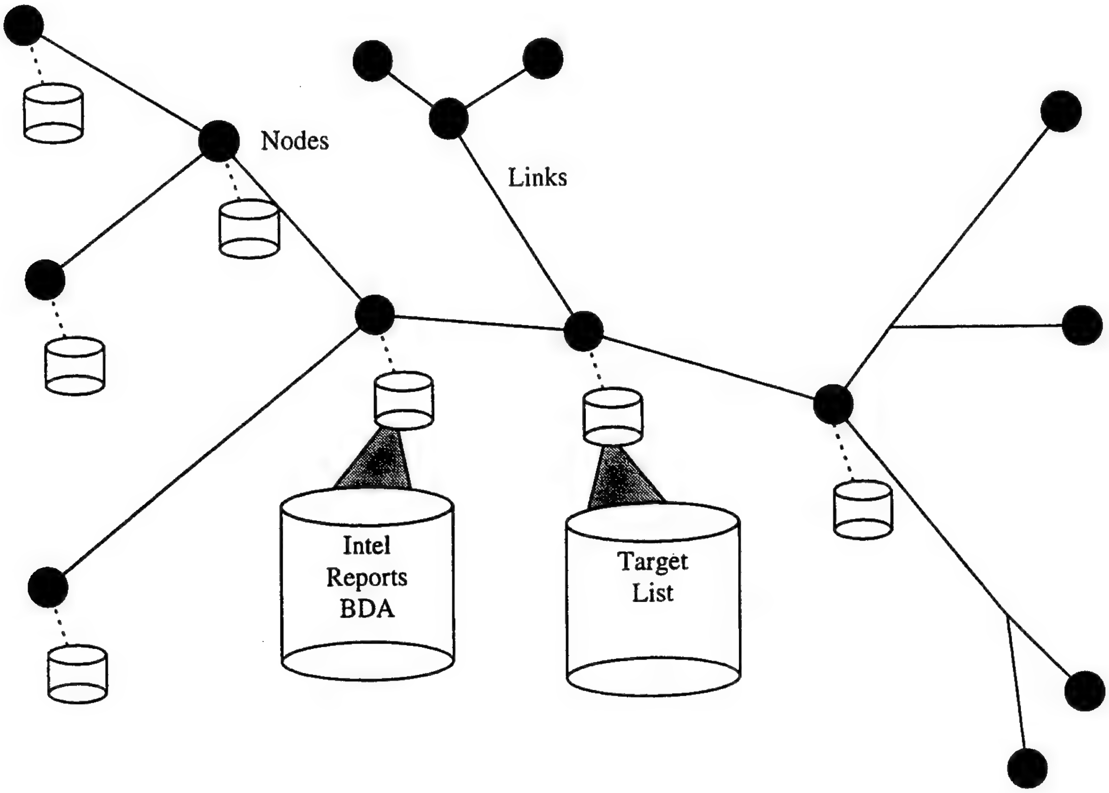


Figure 6-3 - Information Value Model

In Figure 6-3, many of the nodes are computer systems or are dependent upon computer systems and supporting databases. These databases are used as information passes through the network to add value. Information-based processes using the network cannot proceed unless this information is present and available. Some information-based processes will also require that the data-in the IVM, is not only present, but is also up-to-date.

Information will be represented in meaningful levels of detail to show significant databases, intelligence, logistics, etc. which is required for an information-based operation. The IVM will allow the review of the impact of losing a specific component of information (at a granular level, as defined by the IVM implementation).

The recommended initial implementation of the IVM is to concentrate on information dependency. For example, indicating that node A includes a database which could be required by an information-based process. Modeling of the actual data content, how it affects an operation, in a generic way will occur at a later time. While it will be useful to indicate that, for example, a specific intelligence flow depended on a given set of records in a database, implementation of this level of detail is not practical. From a defensive IW point of view, an attack is likely to be a denial of service attack and directed at a database as a whole. In addition, data within a computer system is typically protected at the same level . A security weakness threatens all data on a system, and it is, therefore, reasonable to assume that once a threat has successfully invaded a system, it is equally likely to destroy one database as another.

Eventually, the IVM will support generic modeling of data value at a finer level of detail. Perhaps the most dangerous form of IW is not destroying data, but rather selectively and covertly changing data. If the IVM supported analysis at this level, tools could be developed to assess what changes will be the most destructive to operations and therefore the user could perhaps institute security to guard against them. Modification of data is a form of both tactical deception and psychological operations. The IVM could therefore be used to assess the impact of these activities on an operation. This will be a very valuable capability which should be examined when threats progress to the point where data modification is possible.

The IVM primarily defines the location and basic description of the data. There is not a dependency model. Data is not viewed to be dependent upon other data. These relationships will be represented within the IFM. The IFM will define the fact that a given process or data item in a process depends upon timely update of other data.

6.4.3 Information Flow Model (IFM)

IFM builds upon the ICM and IVM to define the process of information flowing through a network. The IFM defines a class named an ***information flow template*** which represents the information flow for a given operation. This template defines the path of the information (using the ICM), the data upon which it depends (using the IVM), and adds attributes defining the flow and expected delivery time. The IFM defines the dynamic information dependencies which state that a given piece of information must be available or else the process cannot continue. The IFM can also capture dependencies such as requiring data to be up to date before the process can continue.

An information flow template is constructed as a feedback loop. This is because information-based processes require feedback (such as BDA). Information-based processes can be affected either through their primary flow or their feedback flow. Information-based processes are typically repetitive and cannot repeat unless feedback for the previous operation is received. An information flow template is similar with an OODA loop. Figure 6-4 illustrates the basic IFM concept.

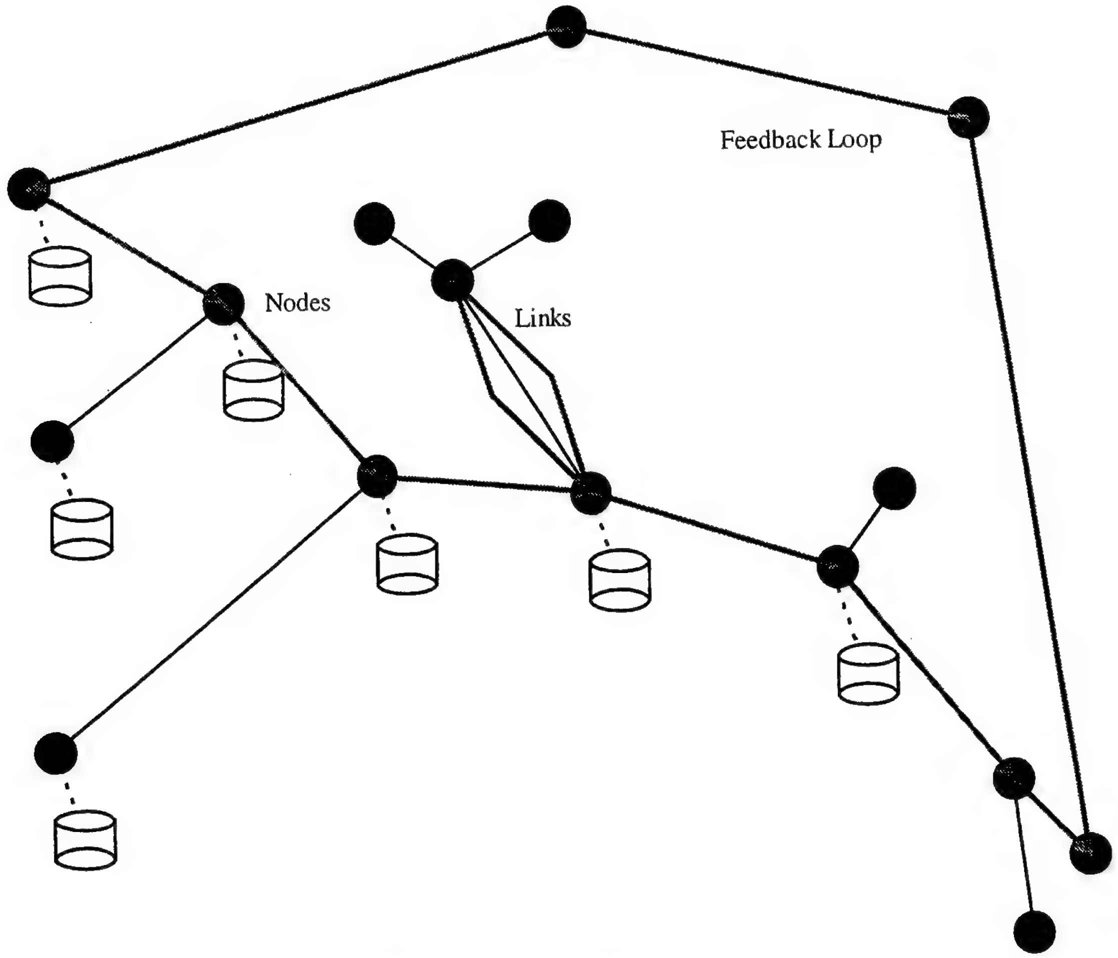


Figure 6-4 - Information Flow Model

The level of detail expressed within the IFM is up to the user. The IFM is intended to be maintained at a level of detail that will not exceed that of the ICM and IVM (you can only define flows which connect objects defined in the ICM/IVM). Flows can be varying levels of detail. For example, the primary forward flow may be specified at a detailed level and the feedback flow may be much simpler.

Some work has been performed in this area, particularly in the area of C2. C2 databases such as CONSTANT WEB, provide detailed hierarchies of C2. C2 is a primary (but not the only) information flow which needs to be represented. Other flows include intelligence, targeting, ATO generation, logistics, etc.

As described, there will be many information flows within an area of operation. The IFM will allow the user to build modular information flow templates. The concept is to allow the user to build any number of information flows and allow their interconnection to define the larger process. The capability provided is that the inter-relationships of various process flows, and the dependencies they create can be examined. This will allow a variety of applications including determining how a coordinated, but individually subtle attack could seriously interrupt an information flow. Figure 6-5 illustrates the concept of a hierarchy of information flows.

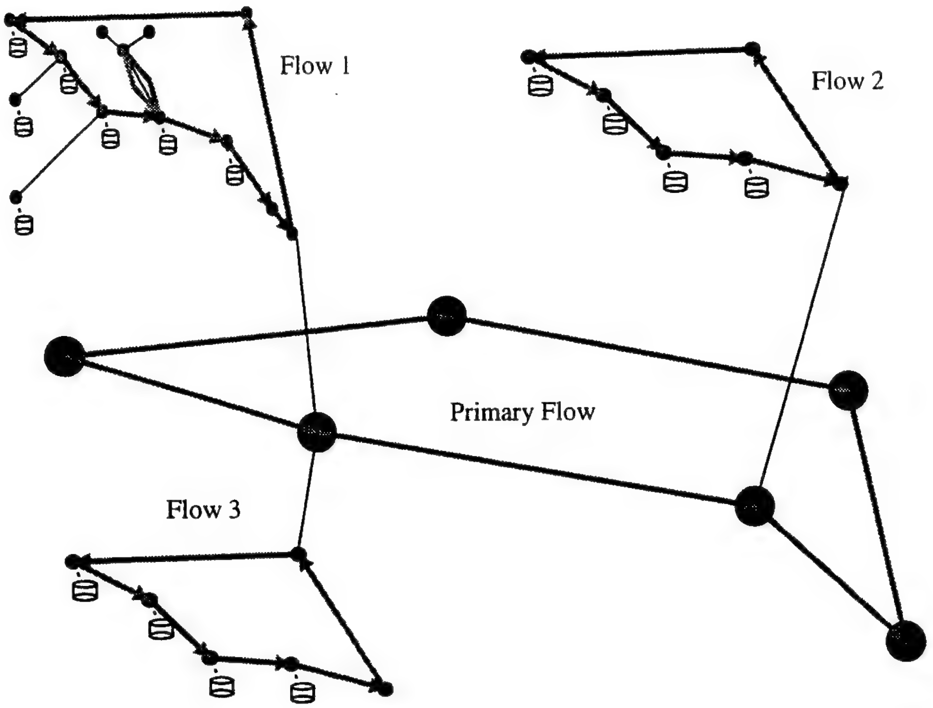


Figure 6-5 - Multiple Information Flows

The concept is that there are many interconnected information flows in an operation and subtle attacks on different flows can have a serious negative impact on an operation. As an example, an apparently insignificant attack on a relatively obscure information flow (Flow 1) could disable primary information flow. The IFM will be designed to allow the user to understand the relationships and identify likely points where an effective attack could take place.

6.5 Threat Models

In order to realistically identify vulnerabilities to the network, the potential threats must be modeled. The threats will be represented and modeled at a functional level of fidelity consistent with the data and attributes specified within the ICM. Developing threat models is preferable as opposed to allowing the user to simply designate a node or link as disabled. The library of threat models will provide the user with a "palette" which will be used to simulate various IW attacks on the network and review the results. The library of threat models will also be used by an automated vulnerability identification tool to match threats to likely targets.

The threat models will consist of "hard kill" threats which permanently disable a node or link and "soft kill" threats which temporarily jam, degrade, or destroy information.

Due to the focus of the IW modeling tool on computers in the network, threats designed to attack information (such as viruses) will be designed to realistically traverse the network based upon presence of security weaknesses on multiple computer systems. The ICM will include security information such as external network access, firewall, operating system, and known vulnerabilities. Threats which depend upon these vulnerabilities will traverse the network and realistically attack multiple nodes.

6.6 Tool Description

The IW modeling tool will consist of a collection of applications which will be used to provide access and simulation using the information and threat models. Figure 6-6 provides a high level data flow for the IW modeling tool.

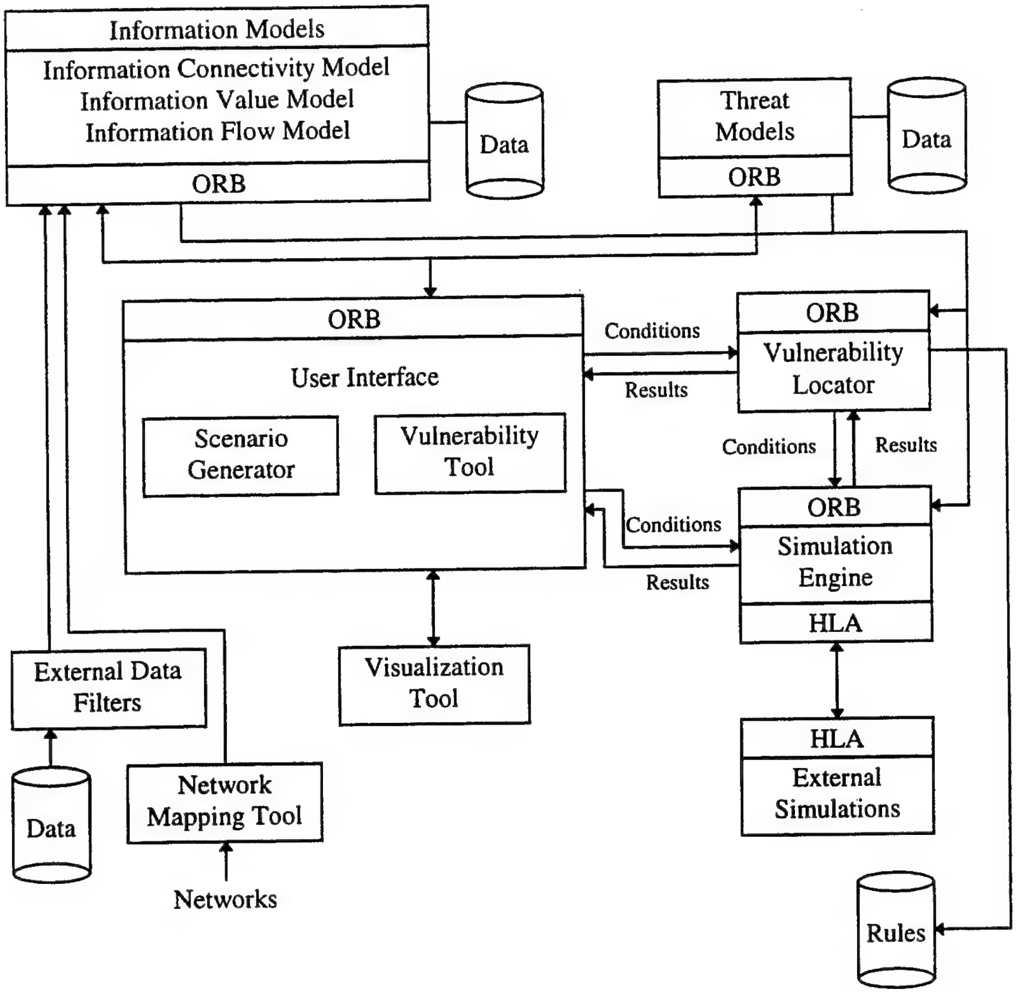


Figure 6-6 - IW Modeling Tool Data Flow

The IW modeling tool is divided into the information/threat models, the user interface processes, and background processes. The implementation of these functions will depend upon the availability of existing components. The system is assumed to use the Unix operating system, using C++ for new software development, using X Windows/Motif for the GUI, and a Common Object Request Broker Architecture (CORBA) compliant ORB to manage access to distributed objects (such as the information and threat models and data).

Each of these functions is described further in the following sections.

6.6.1 Information and Threat Models

The Information (ICM, IVM, and IFM) and threat models represent the core models of the system. The models will be represented as C++ objects, which will be accessed through an ORB. The data for various user scenarios will be stored with a database. The implementation of the database will depend upon the availability of existing data.

6.6.2 User Interface

The IW modeling tool will consist of a controlling application which provides a GUI. The implementation of the GUI will depend on which components can be obtained and reused. The user interface will consist of a visualization tool, scenario generation tools, and front-end user interfaces for the simulation engine and vulnerability identification processes.

The following section describes the major functions provided by the GUI.

6.6.2.1 Visualization

The primary user interface for the IW modeling tool is a common visualization/mapping tool. The visualization tool is expected to be used for all network display applications including information model display, scenario generation, and simulation. Using the same interface for all functions will simplify use for the user.

A key to performing defensive or offensive IW is understanding the network and the assets for which a user is responsible. Because the data in the ICM is, for the most part, arranged geographically, a map-based tool is required to display the spatial relationships of the data. There is also data present in the Information Model which is not truly geographic, but can be well represented with a spatial display.

The visualization tool can either be loosely or tightly coupled with the other processes comprising the GUI. A tightly coupled tool is one in which the visualization capabilities are integrated with other functions typically within one executable. A loosely coupled (application-independent) tool is one which is a separate executable and provides a documented Application Programming Interface (API) used to display objects in the tool. The NSA's OILSTOCK tool and Rome Laboratory's Spatial Display Tool (SDT) are standard visualization tools which implement this paradigm. This approach offers the following advantages:

- An existing map tool can be leveraged.
- Visualization functions can be isolated from application services.
- A standard, familiar tool can be used.
- Other applications using the tool can be quickly integrated.

The major problem with a loosely coupled visualization tool is that highly interactive applications will have a difficult time interfacing with it. The API is normally simplistic and applications of the visualization tool are limited by the available functionality. Despite this, due to the large existing investment in visualization/mapping tools, an existing tool should be used for the IW modeling tool.

Ideally, the visualization tool will support multiple windows to allow the user to obtain several views into the Information Model and how it is interacting. The multiple views will be supported for all of the modes. This is an important capability because the user will often need to view threats as they affect widely separated parts of the network. The user will need to see a detailed view of different parts of the network, which will not be possible with a single view. Figure 6-7 illustrates the visualization tool.

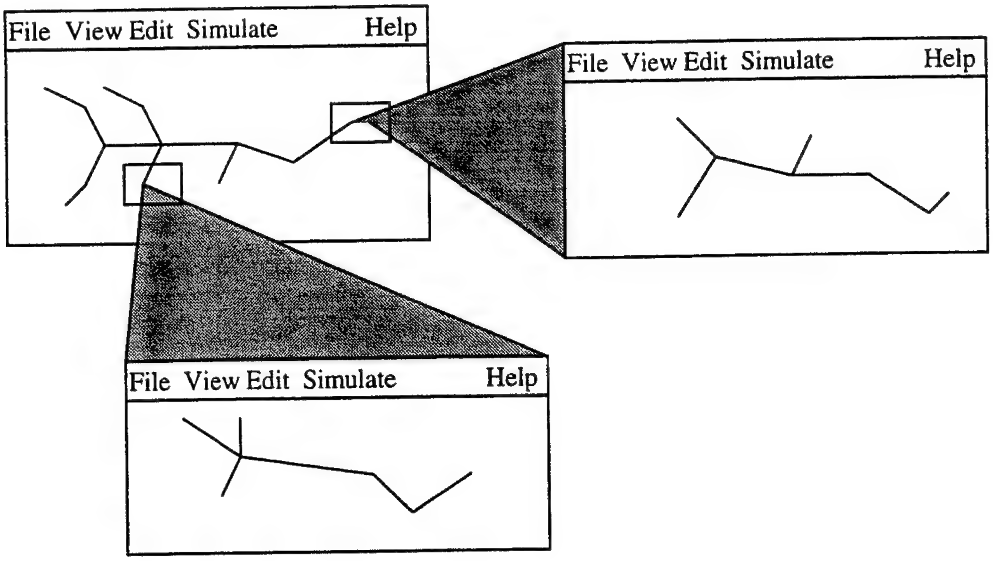

File View Edit Simulate Help
File View Edit Simulate Help
File View Edit Simulate Help

Figure 6-7 - Visualization Tool

As shown in Figure 6-7, the visualization tool will allow the user to obtain multiple views of the network. This will allow the user to have a set of hierarchical views in which each child view is constrained to a portion of its parent view. For this mode, the parent view will include a bounding box that shows the area of the network that a child view is constrained.

In addition, the tool will provide a set of filters which allows the user to enable and disable view of various categories of assets within the network. For example, the electrical power, computers, RF links, fiber links, process flow, and data could be defined into categories and enabled or disabled as required.

The visualization tool is expected to support primarily 2-D visualization. 2-D visualization is viewed as sufficient for reviewing the networks. The combination of sub views and hierarchical displays should allow the user to maintain understanding of the data.

6.6.3 Scenario Generation

The scenario generation tool is used to create and maintain the Information Model databases for specific user scenarios. A key to the usability of the IW modeling tool is the ease in which new scenarios can be introduced. The tool must allow rapid, point-and-click and text based input of data. The tool must also allow leveraging off of (inheriting) work already created. This tool will provide GUI screens which are integrated with the visualization tool. Figure 6-8 illustrates the GUI for the scenario generation tool.

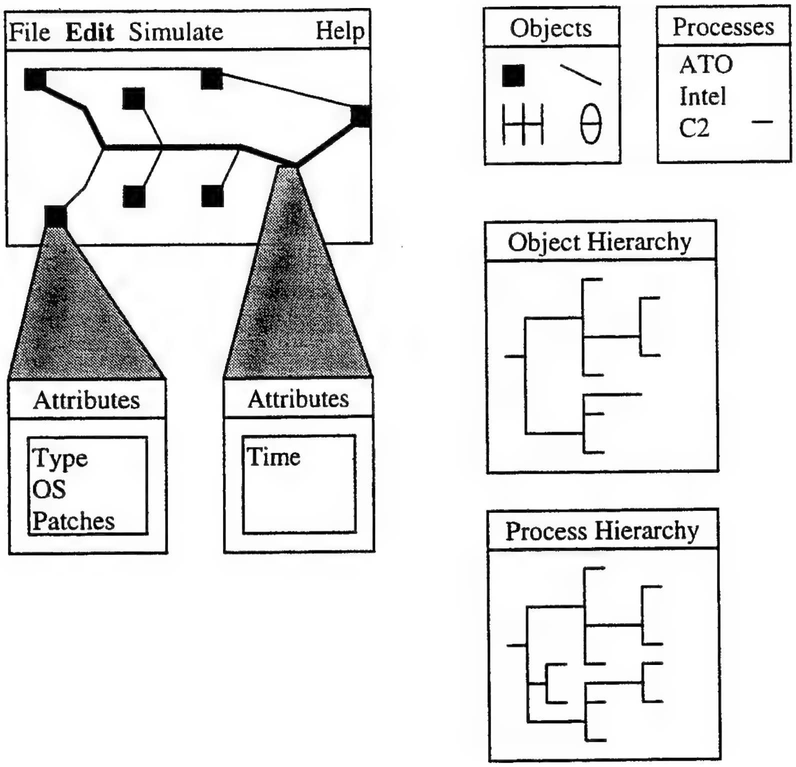


Figure 6-8 - Scenario Generation

The Scenario Generation tool will allow the user to graphically select and "drag and drop" Information Model (ICM, IVM, and IFM) objects into the viewing area to establish the network and information flows. Objects include nodes, computers, links, etc. as defined by the Information Model. The user will also be allowed to group objects and information flows and save them as templates which can be reused. Note that although the Information Model defines the ICM, IVM, and IFM as separate models, the user will edit data for a scenario in a way where the ICM and IVM are treated as objects and the IFM is treated as processes using the network.

As objects are created in the view area, they will inherit default values. The user will be able to click on objects and be provided a dialog which allows completion of the object attributes.

An additional capability will be a dialog which shows the hierarchy of inheritance among templates in the network. This will assist the user in manipulating the network and copying common components.

Once data for the ICM and IVM is input (the network and information), IFM information flow templates can be created by rapidly dragging the mouse through the relevant portions of the network. The user will then be allowed to input information flow attributes. As information flow templates are created, they will be saved for later use and reference.

After the editing process, simple validation checks will be performed to verify that required data is present, all required connections are made, and that the network structure is sensible.

The scenario generation tool will also include filters which convert and insert data from existing databases. This capability will allow rapid creation of networks which can be completed to define a final scenario. Another useful capability will be a tool which can automatically map a network and generate the databases required for the Information Model. Availability of such a tool will simplify Information Model database maintenance and insure that the database is up to date.

6.6.4 Manual Vulnerability Identification

The user interface will also allow the user to manually and automatically identify vulnerabilities in the network. In manual mode, the user will be allowed to drag/select from the available threats and associate a threat with an object in the network (if this makes sense from a vulnerability point of view). The user will also be allowed to associate multiple threats to different objects in the network. Once threats have been associated and positioned in the network, a simulation will take place to identify the impact to the information flow within the network. Figure 6-9 illustrates the threat association process.

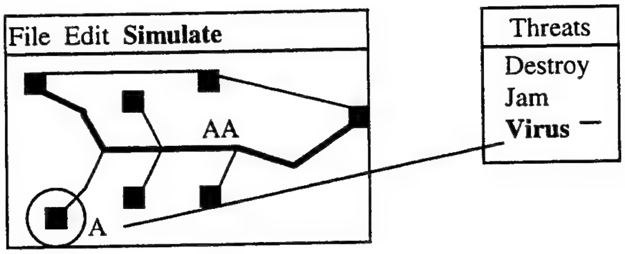
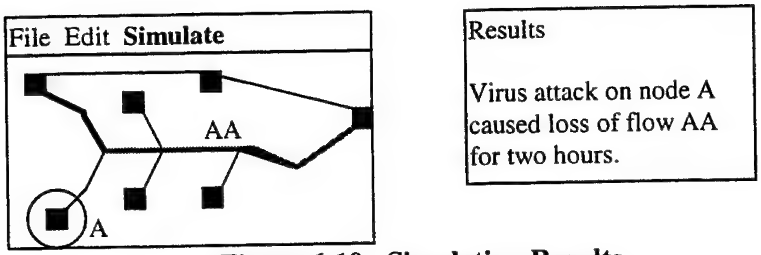


Figure 6-9 - Manual Vulnerability Identification

In addition to manual specification of threats, the user will also be able to indicate a result (or consequence) and have the IW modeling tool identify the possible threats which could cause the identified result (or results).

6.6.5 Simulation Engine

The simulation engine is used to simulate the flow of information, as defined by the information flows, through the ICM. The simulation will be a simple discrete event process in which the flow of information along nodes is timed and attacked nodes affect the process by forcing the information flow to use less efficient communication paths. If the attack occurs to an object for which there is no backup, then the information flow halts until the information or object can be restored. The results of the simulation will be displayed both graphically on the network and textually. Figure 6-10 illustrates the user interface.



Virus attack on node A caused loss of flow AA for two hours.

Figure 6-10 - Simulation Results

The simulation engine will likely be a COTS package, but due to its initial simplicity, could also be quickly implemented with custom software.

The simulation described will inform a user that given attack by specific threats, that certain information flows will be cut off or delayed by a reported amount of time. The simulation will not be able to assess the operational impact of these situations. The user will still be responsible for determining that, for example, a 10 minute delay in a given information flow is an acceptable or unacceptable condition. A second generation simulation will involve a limited fidelity model which simulates a conflict/operation at a campaign level. The simulated IW attack will be introduced as described above, except that the simulation will be integrated into a larger simulation which models a campaign-level operation. The larger simulation will be an end-to-end closed loop model which will be run with an optimal information flow and then with a degraded information flow due to user-defined IW attack conditions. The model will report differences in terms of reduced combat effectiveness due to loss or delay of information flows. This simulation will give a user a quantifiable means of assessing an IW attack.

This simulation will also allow the introduction of multiple attacks to understand the impact to the overall operation. In essence, what this will provide is the ability to manipulate the individually modeled information flows (or OODA loops) and view the effects. An analogy is a set of tuning knobs, one for each OODA loop, which can be manipulated (sped up or down) to determine the overall impact in an operation.

6.6.6 Vulnerability Identification

In addition to manual identification of threats, the IW modeling tool will provide a process whereby the user can enter a set of results and the vulnerability identification process will identify which threats will create that situation. This process will result in a sorted report which identifies the threat conditions that could, as closely as possible, create the user-defined result. The user will also be able to replay each of these conditions to view the result.

This process can use a "brute force" Monte Carlo approach in which threats are systematically applied to objects and then the simulation executed to provide a result. This process can be repeated many times to identify vulnerability conditions. As runs are made, a rule base will be constructed for the scenario which will be used in the future for vulnerability identification runs.

The rule base created will also be available for export to other applications interested in using the Information Model for other purposes.

6.7 Implementation Plan

This section briefly describes a plan for implementation of the IW modeling tool. Initially, a prototype will be developed to verify proof-of-concept. This effort will involve the following major tasks:

- Obtain a set of high level requirements.
- Examine tools upon which the prototype can be based (e.g. OPNET, COMNET).
- Perform a high level system design.
- Develop the information model:
    - Examine existing data models and structures.
    - Examine existing defensive IW databases.
    - Develop an initial, limited model consisting of the ICM, IVM, and IFM with a single Measure of Effectiveness (MOE).
    - Populate the model with several simple, but realistic scenario databases.
- Develop a limited set of threat models.
- Develop the user interface tools:
    - Examine existing visualization tools (e.g. SDT and OILSTOCK).
    - Develop the main user interface.
    - Develop a simple scenario generator.
    - If an existing database is used, develop a single filter for this data.
    - Develop the user interface for vulnerability identification.
    - Develop the user interface for simulation results display.
- Obtain or develop a simulation engine.
- Develop a simple "brute force" vulnerability identification process.

The prototype tool will be demonstrated to several potential users including the AFIWC and other organizations. After the initial prototype demonstrations, the following major tasks will be performed:

- Enhance the information model with additional attributes.
- Research and develop a means of automatically generating ICM (network map) information.
- Develop additional, more robust threat models.
- Enhance the scenario generator to include full functionality and data filters.
- Develop a more intelligent vulnerability identification process.
- Integrate into a larger simulation to allow review of IW attacks on overall operations.
- Develop interfaces to other major programs.

6.8 Potential Uses

The IW modeling tool could be used throughout the Air Force and DoD for organizations interested in defensive IW. In addition, the IW modeling tool could be of immediate use to the AFIWC within the context of the following larger systems:

- Information Protect 21 (IP21) - IP21 is the AFIWC's concept for a system that would identify computer-based threats and assist users in countering the attack. The IW modeling tool could be integrated into the IP21 system as the risk analysis/simulation component. A decision support tool such as the IW modeling tool could be used off-line to generate a rule base for planned responses. The IW modeling tool could also be used as a real-time decision aid in determining responses to unanticipated threats.

- IW Initiative (IWI) - The IWI is the AFIWC's integrated set of tools designed to assist in offensive IW/C2W decision making. The IWI consists of a set of tools and models which will be used to identify C2W adversary targets. The IW modeling tool could exist as a model within the IWI or it could perhaps be used as a high level model which identifies initial targets for subsequent analysis with higher fidelity models.

MISSION
OF
ROME LABORATORY

Mission. The mission of Rome Laboratory is to advance the science and technologies of command, control, communications and intelligence and to transition them into systems to meet customer needs. To achieve this, Rome Lab:

a. Conducts vigorous research, development and test programs in all applicable technologies;

b. Transitions technology to current and future systems to improve operational capability, readiness, and supportability;

c. Provides a full range of technical support to Air Force Material Command product centers and other Air Force organizations;

d. Promotes transfer of technology to the private sector;

e. Maintains leading edge technological expertise in the areas of surveillance, communications, command and control, intelligence, reliability science, electro-magnetic technology, photonics, signal processing, and computational science.

The thrust areas of technical competence include: Surveillance, Communications, Command and Control, Intelligence, Signal Processing, Computer Science and Technology, Electromagnetic Technology, Photonics and Reliability Sciences.